Claims

1.-5. (cancelled)

6. (new) A method for generating and/or validating electronic signatures, the method comprising:

generating an asymmetrical key pair which includes a private signature key and a public validation key;

calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function; and

performing a certification of the public validation key.

7. (new) The method according to Claim 6, wherein, when validating, only those signatures which are and/or were generated at a time prior to the certification of the public validation key are recognized as valid.

8. (new) The method according to Claim 6, wherein, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key.

9. (new) The method according to Claim 7, wherein, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key.

10. (new) The method according to Claim 8, wherein an implementation of the reference is performed by a calculation of a hash value for the electronic document.

11. (new) The method according to Claim 9, wherein an implementation of the reference is performed by a calculation

of a hash value for the electronic document.

12. (new) The method according to Claim 6, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

13. (new) The method according to Claim 7, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

14. (new) The method according to Claim 8, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

15. (new) The method according to Claim 9, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

16. (new) The method according to Claim 10, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

17. (new) The method according to Claim 10, wherein, following calculation of the signature and prior to its transfer to a

recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

18. (new) A method for generating and/or validating electronic signatures, the method comprising:

generating an asymmetrical key pair which includes a private signature key and a public validation key;

calculating at least one electronic signature for at least one electronic document by means of the private signature key and by applying a predeterminable signature function; and

following calculation of the electronic signature, of which there is at least one, carrying out a certification of the public validation key.

19. (new) The method according to Claim 18, wherein, when validating, only those signatures which are and/or were generated at a time prior to the certification of the public validation key are recognized as valid.

20. (new) The method according to Claim 18, wherein, when certifying the public validation key, at least one reference to the electronic document, of which there is at least one, is included in addition to a user identifier and the public validation key.

21. (new) The method according to Claim 19, wherein, when certifying the public validation key, at least one reference to the electronic document, of which there is at least one, is included in addition to a user identifier and the public validation key.

22. (new) The method according to Claim 20, wherein an implementation of the reference, of which there is at least

one, takes place by means of a calculation of a hash value for the electronic document, of which there is at least one.

23. (new) The method according to Claim 18, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, of which there is at least one, in order to verify an action of intent which is expressed by the electronic document, of which there is at least one.